UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/727,274	12/02/2003	Simon Robert Walmsley	PEA18US	4549

24011 7590 08/07/2008

SILVERBROOK RESEARCH PTY LTD
393 DARLING STREET
BALMAIN, 2041
AUSTRALIA

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
08/07/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/727,274	WALMSLEY, SIMON ROBERT	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 June 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on June 11, 2008 has been entered. Claims s 1, 2, 10 have been amended. Claims 1-15 are pending and have been considered below.

Response to Arguments

2. Applicant's arguments filed 06/11/2008 have been fully considered but they are not persuasive. Applicant argued that "It is respectfully submitted that the subject matter of amended independent claims 1, 2 and 10, and claims 3-9 and 11-15 dependent therefrom, is not disclosed by Collins, because Collins specifically discloses that exclusive OR functions are not suitable for the combination process 504 (see col. 9, lines 7-9), and in any case, does not disclose or suggest to applying a combination of exclusive OR and one-way functions, as required by the claimed invention"

3. The examiner respectfully disagrees and submits that Collins discloses a step of Generating an authentication code on the basis of the action and a parameter by applying a combination of exclusive OR and one-way functions to the action and parameter (See column 10, lines 44-57: Fig. 6b, item 1002*) when both confidentiality*

and integrity of the message are required, the secret message value 506 is combined with a MAC variant 1000 in an XOR process 1002 to output and integrity secret message value 1008).

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-15 are rejected under 35 U.S.C. 102(e) as being anticipated by Collins (US 7,095,855).

Claim 1: Collins discloses a message a method of generating and sending a message from a first entity, the method including the steps of:

i. Determining a message including an action (*column 1, line 49-55, column 6, lines 4-36*);

ii. Generating an authentication code on the basis of the action (*application*) and a parameter (*application identifier*) by applying a combination of exclusive OR and one-way functions to the action and parameter, the parameter being indicative of an attribute of the action the (*The message unique value 502 is combined with the secret value 400 in*

combination process 504 to form a secret message unique value 506. The secret message unique value 506 is unique to the particular message, device and application. The combination process 504 can be implemented using the symmetric encryption based one way functions used in the financial industry, and/or hash functions such as SHA-1 and MD5) (column 1, lines 55-62; column 2, lines 34-42; column 3 lines 15-22; column 5, line 57 to column 6 line 4; column 10, lines 44-57: Fig. 6b, item 1002); and

iii. Sending the message and authentication code from the first entity (*to form a secure message for transmission) (column 1 lines 63-67*).

Claim 2: Collins discloses a message a method of generating and sending a message from a first entity, the method including the steps of:

i. Determining a message including an action (column 1, line 49-55, column 6, lines 4-36);

ii. Generating an authentication code on the basis of the action (*application*) and a parameter (*application identifier*) by applying a combination of exclusive OR and one-way functions to the action and parameter, the parameter being indicative of an attribute of the action the (*The message unique value 502 is combined with the secret value 400 in combination process 504 to form a secret message unique value 506. The secret message unique value 506 is unique to the particular message, device and application. The combination process 504 can be*

implemented using the symmetric encryption based one way functions used in the financial industry, and/or hash functions such as SHA-1 and MD5) (column 1, lines 55-62; column 2, lines 34-42; column 3 lines 15-22; column 5, line 57 to column 6 line 4; column 10, lines 44-57: Fig. 6b, item 1002); and

iii. Sending the message and authentication code from the first entity (*to form a secure message for transmission) (column 1 lines 63-67*).

Claims 3/1, 3/2: Collins discloses a message a method of generating and sending a message from a first entity as in claims 1 and 2 above, and further discloses that the action (*application*) is a function, and the parameter (*application identifier*) is indicative of the function (*each communication type is associated with a particular application in the issuer device and a corresponding application in the holder device) (column 5 line 57 to column 6 line 4*).

Claims 4/1, 4/2: Collins discloses a message a method of generating and sending a message from a first entity as in claims 3/1 and 3/2 above, and further discloses that the entity is capable of generating messages for each of a plurality of types of function, and the parameter is indicative of the type of function comprised by the message that is sent (*the corresponding applications 206 and 208 are assigned application identity values 406 and 414, to permit identification of an application or purpose for a particular message) (column 7 line 19 to column 8 line 4; Fig 2; Table 1).*

Claims 5/1, 5/2: Collins discloses a message a method of generating and

sending a message from a first entity as in claims 3/1 and 3/2 above, and further discloses that the message includes one or more operands of the function (*column 7 line 19 to column 8 line 4; Fig 2; Table 1*).

Claims 6/1, 6/2: Collins discloses a message a method of generating and sending a message from a first entity as in claims 5/1 and 5/2 above, and further discloses that the function is a read function and the one or more operands include an address to be read (*From a practical perspective, secure communications between the user 1034 and the banking service 1032, are used for transactions ranging from initial log on and password hand shaking between the banking service 1032 and the user 1034, through to other banking transactions such as reading an account balance, transferring funds and so on)(column 12, lines 20-45*).

Claims 7/1, 7/2: Collins discloses a message a method of generating and sending a message from a first entity as in claims 5/1 and 5/2 above, and further discloses that the function is a write function and the one or more operands include data to be written (*column 7, lines 37-45*).

Claims 8/1, 8/2: Collins discloses a message a method of generating and sending a message from a first entity as in claims 4/1 and 4/2 above, and further discloses that the types of function include at least a read and a write, wherein the authentication step produces a different authentication code depending upon whether the action is a read or a write (*column 7 line 19 to column 8 line 4*).

Claims 9/1, 9/2: Collins discloses a message a method of generating and

sending a message from a first entity as in claims 4/1 and 4/2 above, and further discloses that the authentication step produces includes authentication codes (this process can be selected appropriately to provide symmetric key encryption for confidentiality, or for providing a message integrity mechanism, such as message authentication code or keyed hash function or simply as a secret one time value within a higher level protocol) (column 9, lines 30-40).

Claim 10: Collins discloses a method of generating a first authentication code for a first message for a first function, wherein operands for the first authentication function used to generate the first authentication code include at least part of the first message and at least one identifier associated with the first function the first authentication code is generated by applying a combination of exclusive OR and one-way functions to the at least part of the first message and at least one identifier and then encrypting the result (*The message unique value 502 is combined with the secret value 400 in combination process 504 to form a secret message unique value 506. The secret message unique value 506 is unique to the particular message, device and application. The combination process 504 can be implemented using the symmetric encryption based one way functions used in the financial industry, and/or hash functions such as SHA-1 and MD5) (column 1, lines 55-62; column 2, lines 34-42; column 3 lines 15-22; column 5, line 57 to column 6 line 4 column 10, lines 44-57: Fig. 6b, item 1002*).

Claim 11: Collins discloses a method of generating authentication code as in claim 10 above, and further discloses a steps of verifying the authentication code

in accordance with the at least one identifier associated with the first function (*If the encoding process 602 (see FIG. 6) implemented a message integrity mechanism such as a MAC or keyed hash function, then the decoding process 900 verifies the integrity of the secret message block 604 against message corruption or tampering, using MAC or keyed hash techniques, or both, as applicable) (column 11, lines 25-40)*.

Claim 12: Collins discloses a method of generating authentication code as in claim 10 above, and further discloses that the identifier is indicative of a type of the function (*the corresponding applications 206 and 208 are assigned application identity values 406 and 414, to permit identification of an application or purpose for a particular message) (column 7 line 19 to column 8 line 4; Fig 2; Table 1*).

Claims 13, 14: Collins discloses a method of generating authentication code as in claims 10 and 12 above, and further discloses that the at least one identifier is indicative of the entity generating the authentication code *(addition, the authentication information can be used as a basis for establishing the origin, destination, sequence and timing of messages) (column 6, lines 14-35*).

Claim 15: Collins discloses a method of generating authentication code as in claim 14above, and further discloses that prior to generating the authentication code, of receiving a request from the entity for the first message, the request including information indicative of an identity of the entity *(as a prerequisite to answering the request, a reliable indication that the information request has*

originated from a device and/or application which is known to, and authorized by, the information provider)(column 6, lines 1-35).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
Friday, August 01, 2008

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2136